

BS ISO/IEC 13888-2:2010

Incorporating Corrigendum December 2012



BSI Standards Publication

Information technology — Security techniques — Non-repudiation

Part 2: Mechanisms using
symmetric techniques

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 13888-2:2010, incorporating Corrigendum December 2012. It supersedes BS ISO/IEC 13888-2:1998, which is withdrawn.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum December 2012 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013.
Published by BSI Standards Limited 2013.

ISBN 978 0 580 79131 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2011.

Amendments/corrigenda issued since publication

Date	Text affected
31 January 2013	Implementation of ISO/IEC corrigendum December 2012

**Information technology — Security
techniques — Non-repudiation —**

**Part 2:
Mechanisms using symmetric techniques**

*Technologies de l'information — Techniques de sécurité — Non-
répudiation —*

Partie 2: Mécanismes utilisant des techniques symétriques



Reference number
ISO/IEC 13888-2:2010(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2010

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	3
5	Notation	3
5.1	Notation from ISO/IEC 13888-1	3
5.2	Notation unique for the purposes of this part of ISO/IEC 13888	4
6	Requirements.....	4
7	Secure envelopes	5
8	Generation and verification of non-repudiation tokens	5
8.1	Creation of tokens by the TTP	5
8.2	Data items used in the non-repudiation mechanisms	5
8.3	Non-repudiation tokens	6
8.4	Verification of tokens by the TTP	7
9	Specific non-repudiation mechanisms	8
9.1	Mechanisms for non-repudiation.....	8
9.2	Mechanism for non-repudiation of origin	8
9.3	Mechanism for non-repudiation of delivery.....	9
9.4	Mechanism for obtaining a time stamping token.....	10
Annex A	(informative) Examples of specific non-repudiation mechanisms	11
A.1	Examples of non-repudiation mechanisms of origin and delivery	11
A.2	Mechanism M1: Mandatory NRO, optional NRD	11
A.3	Mechanism M2: Mandatory NRO, mandatory NRD	13
A.4	Mechanism M3: Mandatory NRO and NRD with intermediary TTP	14
	Bibliography.....	17

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 13888-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 13888-2:1998), which has been technically revised.

ISO/IEC 13888 consists of the following parts, under the general title *Information technology — Security techniques — Non-repudiation*:

- *Part 1: General*
- *Part 2: Mechanisms using symmetric techniques*
- *Part 3: Mechanisms using asymmetric techniques*

Information technology — Security techniques — Non-repudiation —

Part 2: Mechanisms using symmetric techniques

1 Scope

The goal of the non-repudiation service is to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. This part of ISO/IEC 13888 provides descriptions of generic structures that can be used for non-repudiation services, and of some specific communication-related mechanisms which can be used to provide non-repudiation of origin (NRO) and non-repudiation of delivery (NRD). Other non-repudiation services can be built using the generic structures described in this part of ISO/IEC 13888 in order to meet the requirements defined by the security policy.

This part of ISO/IEC 13888 relies on the existence of a trusted third party (TTP) to prevent fraudulent repudiation or accusation. Usually, an online TTP is needed.

Non-repudiation can only be provided within the context of a clearly defined security policy for a particular application and its legal environment. Non-repudiation policies are defined in ISO/IEC 10181-4.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9798-1:1997, *Information technology — Security techniques — Entity authentication — Part 1: General*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

ISO/IEC 13888-1, *Information technology — Security techniques — Non-repudiation — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 13888-1 and the following apply.

3.1

cryptographic check function

cryptographic transformation which takes as input a secret key and an arbitrary string, and which gives a cryptographic check value as output

[ISO/IEC 9798-1]

3.2

data integrity

property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

3.3

evidence generator

entity that produces non-repudiation evidence

[ISO/IEC 10181-4]

3.4

hash-function

function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

- it is computationally infeasible to find for a given output an input which maps to this output;
- it is computationally infeasible to find for a given input a second input which maps to the same output

[ISO/IEC 10118-1]

3.5

key

sequence of symbols that controls the operations of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check-function computation, signature calculation, or signature verification)

[ISO/IEC 11770-1]

3.6

MAC algorithm

algorithm for computing a function which maps strings of bits and a secret key to fixed-length strings of bits, satisfying the following properties:

- for any key and any input string the function can be computed efficiently;
- for any fixed key, and given no prior knowledge of the key, it is computationally infeasible to compute the function value on any new input string, even given knowledge of the set of input strings and corresponding function values, where the value of the i th input string may have been chosen after observing the value of the first $i-1$ function values

[ISO/IEC 9797-1]

3.7

message authentication code

MAC

string of bits which is the output of a MAC algorithm

[ISO/IEC 9797-1]

NOTE A MAC is sometimes called a cryptographic check value (see for example ISO/IEC 7498-2).

3.8

secret key

key used with symmetric cryptographic techniques and usable only by a set of specified entities

[ISO/IEC 11770-1]